**Security+ Bonus Exam 4**

65 Questions

1. RBAC manages access by using \_\_\_\_\_\_\_\_\_\_.

A. User identity

B. Security domains

C. Job descriptions

D. Sensitivity levels

2. A smart card is an example of what type of authentication factor?

A. “Something you have”

B. “Something you are”

C. “Something you know”

D. “Something you do”

3. Which of the following is not true in regard to Kerberos?

A. Provides end-to-end security

B. Is not scalable

C. Uses DES

D. Is a trusted third-party authentication system

4. What form of authentication periodically reauthenticates the client?

A. Kerberos

B. PAP

C. Certificates

D. CHAP

5. Certificates are used for what purpose?

A. Prove reliability

B. Prove compatibility

C. Prove identity

D. Prove timeliness

6. A token is a physical implementation of what?

A. Static password

B. Biometric factor

C. Something you know

D. One-time password

7. In mutual authentication, what occurs?

A. Two clients authenticate simultaneously.

B. A server authenticates to a Kerberos server.

C. The client and the server authenticate to each other.

D. Multifactor authentication is used.

8. What form of attack prevents a server from responding to legitimate requests for resources?

A. Backdoor

B. Impersonation

C. Replay

D. Denial-of-service

9. RADIUS can be used to provide an additional layer of security for the network against \_\_\_\_\_\_\_\_\_\_.

A. Internal users

B. DoS attacks

C. Virus infections

D. Remote users

10. PPTP can use all but which of the following authentication protocols?

A. AH

B. PAP

C. CHAP

D. EAP

11. Which of the following is the biggest issue related to data and resources stored or hosted in a cloud computing solution?

A. Reducing local hardware requirements

B. Allowing for real-time backups

C. Whether or not it is actually securable

D. Enabling anywhere access

12. One of the most popular and widely used email encryption solutions, especially for Internet-based email, is \_\_\_\_\_\_\_\_\_\_.

A. PGP

B. SSH

C. SSL

D. S/MIME

13. The best countermeasure against email spam is \_\_\_\_\_\_\_\_\_\_.

A. Acceptable use policies

B. Filters

C. Blocking attachments at network borders

D. Spoofing email addresses

14. When TLS is being used to secure web communications, what URL prefix appears in the address bar to signal this fact?

A. SHTTP://

B. TLS://

C. SECURE://

D. HTTPS://

15. What network device can be used to create and manage virtual LANs?

A. Switch

B. Router

C. Firewall

D. Proxy

16. A network-based IDS is good at detecting and stopping what form of attack?

A. Spoofing

B. Denial-of-service

C. Spam

D. Buffer overflow

buffer overflow attacks.

17. A host-based IDS is limited by \_\_\_\_\_\_\_\_\_\_.

A. Host auditing capabilities

B. Switched networks

C. Speed of the NIC

D. Encrypted transmissions

18. The best way to respond to security violations is to \_\_\_\_\_\_\_\_\_\_.

A. Notify law enforcement immediately.

B. Turn off all servers.

C. Initiate a lockdown so no employees can enter or leave the facility.

D. Have an incident response plan to follow.

19. When a vendor releases a new service pack, what is the first step you should take?

A. Install it on production systems.

B. Document the changes to the environment.

C. Test it on nonproduction systems.

D. Update user awareness training.

20. What is the central feature of asymmetric cryptography?

A. It is performed in only one direction.

B. The same key that locks can be used to unlock.

C. It is useful for bulk encryption.

D. It has public key/private key pairs.

21. Asymmetric cryptography is said to provide all but which of the following security services?

A. Confidentiality

B. Integrity

C. Authentication

D. Nonrepudiation

22. What dictates what is and what is not acceptable in regard to how certificates can be used and defines a set of rules that control how certificates are used, managed, and deployed?

A. Certificate practice statements

B. OCSP systems

C. Certificate policies

D. Internet standards

23. To provide a level of fault tolerance in encryption and certificate systems, which of the following can be used to recover keys in the event of a key or certificate corruption?

A. Escrow

B. Honey pot

C. IDS

D. VLAN

24. Which of the following can make or break security for an environment?

A. Failing to apply a recent software patch

B. Using guard dogs instead of security guards

C. Not reviewing the audit trails of client systems

D. Lack of physical access control

25. In order to provide the strongest level of security control over a facility, locked doors can authenticate authorized personnel through what means?

A. Metal keys

B. Proximity detectors

C. Biometrics

D. Smart cards

26. \_\_\_\_\_\_\_\_\_\_\_ may be left in an application by developers once a product is released to market. It was originally installed to allow for quick debugging.

A. A Trojan horse

B. A back door

C. An input validation check

D. A quality assurance test

27. All but which of the following are true in regard to a man-in-the-middle attack?

A. It’s a form of eavesdropping attack.

B. It allows the attacker to intercept encrypted communications.

C. It’s easy to perform.

D. It requires the attacker to impersonate the server to the client.

28. A man-in-the-middle attack can possibly be waged by performing which of the following techniques?

A. TCP/IP hijacking

B. Backdoor attack

C. Replay attack

D. Social engineering

29. What is the default service port of SFTP?

A. 21

B. 22

C. 23

D. 25

30. Most password-guessing attacks employ what attack process?

A. Statistical anomaly attack

B. Reverse hash-matching attack

C. Mathematical attack

D. Implementation attack

31. The best protection against known viruses is \_\_\_\_\_\_\_\_\_\_\_.

A. User behavior modification

B. Virus scanners

C. Restriction of Internet downloads

D. Not reusing removable media from other environments

32. What form of malicious code lies dormant until a specific triggering event is encountered?

A. Trojan horses

B. Viruses

C. Logic bombs

D. Worms

33. Which of the following options is the most secured version of wireless configuration?

A. OSA

B. WEP

C. WPA

D. CCMP

34. What type of attack enables a hacker to forcibly send messages to Bluetooth devices?

A. War driving

B. Bluejacking

C. IV attack

D. Bluesnarfing

35. What is the term used to describe the alarm sounded by an IDS (intrusion detection system) based on events it sees in live network traffic that are different from established parameters but which turn out to be benign?

A. True positive

B. False positive

C. True negative

D. False negative

36. A signed message or data indicates what?

A. Its source of origin

B. Its compatibility with your operating system

C. Its reliability

D. Its programming quality

37. LDAP, a standardized protocol that enables clients to access resources within a directory service, is based on what standard?

A. X.509

B. 802.11

C. 160 bits

D. X.500

38. If you need to give anonymous users the ability to upload files to an Internet site but you don’t wish to grant them the ability to access or even see any files that have been deposited, what do you need to install?

A. S/FTP server

B. SSL server

C. Blind FTP server

D. Authenticated FTP server

39. What is the risk calculation metric that measures the number of times an unwanted event might occur within the next year?

A. ALE

B. SLE

C. EF

D. ARO

40. What network device is designed to protect one network from another by filtering traffic?

A. A proxy server

B. A modem

C. A firewall

D. A PBX system

41. A link to the network using a modem has what primary difference from a LAN connection?

A. Ability to share files

B. Speed

C. Access to network printers

D. Use of network services

42. What protocol can be used to assist in monitoring the health of a network and to provide a centralized monitoring capability?

A. SMTP

B. TACACS

C. PPTP

D. SNMP

43. When an investigator discovers a hard drive that might contain evidence related to a criminal investigation, what is used to create an exact duplicate of that storage device?

A. Hashing

B. Bit-stream image

C. Undelete

D. Graceful shutdown

44. When performing system hardening, what is the first step?

A. Install patches and updates.

B. Scan for malicious code.

C. Configure security software.

D. Remove unnecessary elements.

45. Smart cards are often used to store \_\_\_\_\_\_\_\_\_\_\_.

A. Encrypted data files

B. Network account databases

C. Digital certificates

D. User emails

46. Which of the following is not a hashing algorithm?

A. SHA-1

B. RC5

C. MD5

D. MD2

47. What is the most important feature of symmetric cryptography?

A. It operates slowly.

B. It is scalable.

C. It uses a shared secret key.

D. It protects integrity.

48. Which of the following is not a valid key size for AES?

A. 128

B. 168

C. 192

D. 256

49. The benefits of a gas-based fire suppression system include all but which of the following?

A. Can be deployed throughout a facility

B. Will cause the least damage to computer systems

C. Extinguishes the fire by removing oxygen

D. May be able to extinguish the fire faster than a water discharge system

50. The most effective alternate site is \_\_\_\_\_\_\_\_\_\_\_.

A. Proposed

B. Hot

C. Warm

D. Cold

51. Cryptography can be used to provide all but which of the following security features or services?

A. Confidentiality

B. Integrity

C. Availability

D. Non-repudiation

52. Availability is threatened by what form of attack?

A. Smurf

B. Port scanning

C. Eavesdropping

D. Password cracking

53. What is a distinctive benefit in deploying an application aware device as compared to a generic firewall appliance?

A. Traffic filtering

B. NAT services

C. Deep packet inspection

D. Network segmentation

54. \_\_\_\_\_ is a networking storage standard based on IP which can be used to enable location independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.

A. Fibre Channel

B. SAN

C. Thunderbolt

D. iSCSI

55. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the process of adding new employees to the IAM (Identity and Access Management) of an organization. This process is also used when the role or position of an employee changes or when they are awarded additional levels of privilege or access.

A. Reissue

B. On-boarding

C. Background checks

D. Site survey

56. Which of the following is a formal declaration of the security stance, risks, and technical requirements of a link between two organization's IT infrastructures?

A. MOU

B. SLA

C. ISA

D. BPA

57. What form of malware takes a computer system hostage and demands payment in order to release control back to the user?

A. Rootkit

B. Ransomware

C. Trojan horse

D. Logic bomb

58. When a security consultant is performing a penetration test but is not provided a set of logon name and passwords by the target organization, what form of assessment is being performed?

A. Announced test

B. Non-credentialed test

C. White box test

D. Intrusive test

59. What is a common organizational and referencing format used by some NoSQL database options?

A. HTML

B. Java

C. JSON

D. LDAP

60. What is the purpose of BYOD policies mandating storage segmentation?

A. Lock the device when the user fails to provide their credentials after repeated attempts

B. Enable all data and possibly even configuration settings to be deleted from a device remotely

C. Isolate the device's operating system and pre-installed apps from user installed apps and user data

D. Oversee the installed apps, app usage, stored data, and data access on a device.

61. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a type of ICS (industrial control system). An ICS is a form of computer management device that controls industrial processes and machines.?

A. SCADA

B. SAN

C. DNS

D. Fibre Channel

62. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds.

A. Certificates

B. TOTP

C. TPM

D. Trusted OS

63. What is the primary reason to maintain a password history?

A. Monitor account logins

B. Force complexity requirements compliance

C. Provide for legal investigations

D. Prevent password reuse

64. Which of the following depends upon ephemeral keys?

A. Digital certificates

B. Perfect forward secrecy

C. Whole drive encryption

D. Integrity protection

65. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the message sent to a certificate authority from an user or organization to request and apply for a digital certificate.

A. SHA-1

B. OCSP

C. PKI

D. CSR

**Security+ Bonus Exam 4  
Answers & Explanations**

1. RBAC manages access by using \_\_\_\_\_\_\_\_\_\_.

A. User identity

B. Security domains

C. Job descriptions

D. Sensitivity levels

Answer: C

RBAC (role-based access control) uses job descriptions to manage access. Discretionary access control (DAC) uses identity. Media/mandatory access control (MAC) uses security domains and sensitivity levels.

2. A smart card is an example of what type of authentication factor?

A. “Something you have”

B. “Something you are”

C. “Something you know”

D. “Something you do”

Answer: A

A smart card is an example of a “something you have” authentication factor. A biometric is something you are, a password is something you know, and your signature is something you do.

3. Which of the following is not true in regard to Kerberos?

A. Provides end-to-end security

B. Is not scalable

C. Uses DES

D. Is a trusted third-party authentication system

Answer: B

Kerberos is scalable. Kerberos also provides end-to-end security, uses DES (Data Encryption Standard), and is a trusted third-party authentication system.

4. What form of authentication periodically reauthenticates the client?

A. Kerberos

B. PAP

C. Certificates

D. CHAP

Answer: D

CHAP (Challenge Handshake Authentication Protocol) periodically reauthenticates the client. Kerberos, PAP (Password Authentication Protocol), and certificates aren’t designed to periodically reauthenticate the client.

5. Certificates are used for what purpose?

A. Prove reliability

B. Prove compatibility

C. Prove identity

D. Prove timeliness

Answer: C

Certificates are used to prove identity. Certificates can’t and aren’t used to prove reliability, compatibility, or timeliness.

6. A token is a physical implementation of what?

A. Static password

B. Biometric factor

C. Something you know

D. One-time password

Answer: D

A token is a physical implementation of a one-time password. A token isn’t a static password device, it isn’t a biometric factor, and it isn’t something you know.

7. In mutual authentication, what occurs?

A. Two clients authenticate simultaneously.

B. A server authenticates to a Kerberos server.

C. The client and the server authenticate to each other.

D. Multifactor authentication is used.

Answer: C

Mutual authentication means that the client and the server authenticate to each other. Two clients authenticating simultaneously is just a high-performance authentication system. A server authenticating to a Kerberos server is a normal action of a Kerberos realm. Using multifactor authentication is stronger than single factor, but it isn’t necessarily mutual.

8. What form of attack prevents a server from responding to legitimate requests for resources?

A. Backdoor

B. Impersonation

C. Replay

D. Denial-of-service

Answer: D

A denial-of-service (DoS) attack prevents a server from responding to legitimate requests for resources. A backdoor attack gives intruders the ability to bypass security to gain access to a system. Impersonation is when someone assumes the identity of another user. Replay attacks occur when authentication traffic is captured and retransmitted.

9. RADIUS can be used to provide an additional layer of security for the network against \_\_\_\_\_\_\_\_\_\_.

A. Internal users

B. DoS attacks

C. Virus infections

D. Remote users

Answer: D

RADIUS (Remote Authentication Dial-In User Service) can be used to provide an additional layer of security for the network against remote users. RADIUS doesn’t provide protection against internal users, DoS (denial-of-service) attacks, or virus infections.

10. PPTP can use all but which of the following authentication protocols?

A. AH

B. PAP

C. CHAP

D. EAP

Answer: A

AH (Authentication Header) is an authentication protocol of IPSec, not PPTP (Point-to-Point Tunneling Protocol). PPTP can use PAP (Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), or EAP (Extensible Authentication Protocol).

11. Which of the following is the biggest issue related to data and resources stored or hosted in a cloud computing solution?

A. Reducing local hardware requirements

B. Allowing for real-time backups

C. Whether or not it is actually securable

D. Enabling anywhere access

Answer: C

There are serious concerns regarding whether or not cloud computer is secure or even securable. Reducing local hardware requirements, allowing for real-time backups, and enabling anywhere access are less critical concerns than security.

12. One of the most popular and widely used email encryption solutions, especially for Internet-based email, is \_\_\_\_\_\_\_\_\_\_.

A. PGP

B. SSH

C. SSL

D. S/MIME

Answer: A

PGP (Pretty Good Privacy) is a popular and widely used email encryption solution, especially for Internet-based email. S/MIME (Secure/Multipurpose Internet Mail Extensions) is also an email encryption solution, but it isn’t as widely used. SSH (Secure Shell) and SSL (Secure Sockets Layer) aren’t email-specific solutions.

13. The best countermeasure against email spam is \_\_\_\_\_\_\_\_\_\_.

A. Acceptable use policies

B. Filters

C. Blocking attachments at network borders

D. Spoofing email addresses

Answer: B

Email filters are the best countermeasure against email spam. Acceptable use policies and blocking attachments don’t address email spam issues even though they’re valid security measures against other email problems. Spoofing email addresses isn’t a security solution, it’s a form of attack.

14. When TLS is being used to secure web communications, what URL prefix appears in the address bar to signal this fact?

A. SHTTP://

B. TLS://

C. SECURE://

D. HTTPS://

Answer: D

HTTPS:// is the correct prefix for the use of HTTP (Hypertext Transfer Protocol) over TLS (Transport Layer Security). This is the same prefix as HTTP over SSL (Secure Sockets Layer). SHTTP:// is for Secure HTTP, which is a different technology. TLS:// and SECURE:// are invalid prefixes.

15. What network device can be used to create and manage virtual LANs?

A. Switch

B. Router

C. Firewall

D. Proxy

Answer: A

A switch can be used to create and manage virtual large area networks (VLANs). Routers, firewalls, and proxies don’t support VLANs.

16. A network-based IDS is good at detecting and stopping what form of attack?

A. Spoofing

B. Denial-of-service

C. Spam

D. Buffer overflow

Answer: B

A network-based IDS (intrusion detection system) is good at detecting and stopping DoS (denial-of-service) attacks. Host-based IDS, in comparison to network-based IDS, is better at detecting and stopping spoofing, spam, and buffer overflow attacks.

17. A host-based IDS is limited by \_\_\_\_\_\_\_\_\_\_.

A. Host auditing capabilities

B. Switched networks

C. Speed of the NIC

D. Encrypted transmissions

Answer: A

Host-based IDS (intrusion detection system) is limited by the host’s auditing capabilities. Host-based IDS isn’t limited by switched networks, speed of the NIC (network interface card), or encrypted transmissions.

18. The best way to respond to security violations is to \_\_\_\_\_\_\_\_\_\_.

A. Notify law enforcement immediately.

B. Turn off all servers.

C. Initiate a lockdown so no employees can enter or leave the facility.

D. Have an incident response plan to follow.

Answer: D

The best way to respond to security violations is to have an incident response plan to follow. The incident response plan may instruct you to contact law enforcement, turn off servers, or initiate a lockdown, but only if the situation requires such actions.

19. When a vendor releases a new service pack, what is the first step you should take?

A. Install it on production systems.

B. Document the changes to the environment.

C. Test it on nonproduction systems.

D. Update user awareness training.

Answer: C

When a new service pack is released, the first step is to test it on nonproduction systems. Only after successful testing should you document the changes to the environment, install the service pack on production systems, and update the user awareness training program.

20. What is the central feature of asymmetric cryptography?

A. It is performed in only one direction.

B. The same key that locks can be used to unlock.

C. It is useful for bulk encryption.

D. It has public key/private key pairs.

Answer: D

Asymmetric cryptography has a central feature of public key/private key pairs. Asymmetric cryptography is reversible (unlike hashing), and the alternate key must be used to unlock (unlike symmetric). In addition, asymmetric cryptography is suited only for small amounts of data (unlike symmetric).

21. Asymmetric cryptography is said to provide all but which of the following security services?

A. Confidentiality

B. Integrity

C. Authentication

D. Nonrepudiation

Answer: B

Hashing provides integrity. Asymmetric cryptography provides confidentiality, authentication, and nonrepudiation.

22. What dictates what is and what is not acceptable in regard to how certificates can be used and defines a set of rules that control how certificates are used, managed, and deployed?

A. Certificate practice statements

B. OCSP systems

C. Certificate policies

D. Internet standards

Answer: C

Certificate policies dictate what is and what is not acceptable in regard to how certificates can be used. They also define a set of rules that control how certificates are used, managed, and deployed. A certificate practice statement describes how a certificate authority will manage the certificates that it issues. An OCSP (Online Certificate Status Protocol) system is used to query whether a certificate is valid or revoked. Certificate solutions are based on Internet standards, such as X.509, but the standards don’t dictate what is acceptable use for them.

23. To provide a level of fault tolerance in encryption and certificate systems, which of the following can be used to recover keys in the event of a key or certificate corruption?

A. Escrow

B. Honey pot

C. IDS

D. VLAN

Answer: A

Escrow provides fault tolerance for encryption and certificate systems to recover keys in the event of a key or certificate corruption. Honey pots, IDSs (Intrusion detection systems), and VLANs (virtual large area network) aren’t associated with certificates or cryptography.

24. Which of the following can make or break security for an environment?

A. Failing to apply a recent software patch

B. Using guard dogs instead of security guards

C. Not reviewing the audit trails of client systems

D. Lack of physical access control

Answer: D

Without physical access control, there is no security. An environment’s security can be maintained in spite of poor management such as not applying software patches, using the wrong protection solution, or not reviewing all audit trails.

25. In order to provide the strongest level of security control over a facility, locked doors can authenticate authorized personnel through what means?

A. Metal keys

B. Proximity detectors

C. Biometrics

D. Smart cards

Answer: C

Biometrics provide the strongest form of authentication when used for physical access control. Metal keys, proximity detectors, and smart cards aren’t as secure since they can be stolen and used by other people.

26. \_\_\_\_\_\_\_\_\_\_\_ may be left in an application by developers once a product is released to market. It was originally installed to allow for quick debugging.

A. A Trojan horse

B. A back door

C. An input validation check

D. A quality assurance test

Answer: B

A back door may be left in an application by developers once a product is released to market. The back door was originally installed to allow for quick debugging. A Trojan horse is a malicious program disguised as a legitimate program. Input validation checks are protections against buffer overflows; they should remain in an application. Quality assurance tests are improvements to the quality of developed software; they’re part of the development process but aren’t coded into the application.

27. All but which of the following are true in regard to a man-in-the-middle attack?

A. It’s a form of eavesdropping attack.

B. It allows the attacker to intercept encrypted communications.

C. It’s easy to perform.

D. It requires the attacker to impersonate the server to the client.

Answer: C

Man-in-the-middle attacks aren’t easy to perform; they’re complicated and require specialized high-end attack tools. Man-in-the-middle attacks are a form of eavesdropping attack; they allow the attacker to intercept encrypted communications, and they require that the attacker impersonate the server to the client.

28. A man-in-the-middle attack can possibly be waged by performing which of the following techniques?

A. TCP/IP hijacking

B. Backdoor attack

C. Replay attack

D. Social engineering

Answer: A

TCP/IP hijacking is a technique that may be used in some forms of man-in-the-middle attacks. Backdoor attacks, replay attacks, and social engineering aren’t typically associated with man-in-the-middle attacks.

29. What is the default service port of SFTP?

A. 21

B. 22

C. 23

D. 25

Answer: B

TCP port 22 is the default service port of SFTP (SSH FTP/Secure FTP). TCP port 21 is used by plaintext FTP, 22 by telnet, and 25 by SMTP.

30. Most password-guessing attacks employ what attack process?

A. Statistical anomaly attack

B. Reverse hash-matching attack

C. Mathematical attack

D. Implementation attack

Answer: B

Most password-guessing attacks employ the reverse hash-matching attack process. Software exploitation attacks may employ statistical anomaly, mathematical, and impersonation attacks.

31. The best protection against known viruses is \_\_\_\_\_\_\_\_\_\_\_.

A. User behavior modification

B. Virus scanners

C. Restriction of Internet downloads

D. Not reusing removable media from other environments

Answer: B

The best protection against known viruses is a virus scanner. Other valid protection methods include user behavior modification, restriction of Internet downloads, and not reusing removable media from other environments.

32. What form of malicious code lies dormant until a specific triggering event is encountered?

A. Trojan horses

B. Viruses

C. Logic bombs

D. Worms

Answer: C

A logic bomb is a form of malicious code that lies dormant until a specific triggering event is encountered. A Trojan horse is a malicious program disguised as something useful or legitimate. Viruses are programs designed to spread from one system to another through self-replication and to perform any of a wide range of malicious activities. Worms are designed to exploit a single flaw or hole in a system (operating system, protocol, service, or application) and then use that flaw or hole to spread or replicate themselves to other systems with the same flaw.

33. Which of the following options is the most secured version of wireless configuration?

A. OSA

B. WEP

C. WPA

D. CCMP

Answer: D

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is a variant of the Advanced Encryption Standard (AES) and the encryption scheme used in WPA2 (WiFi Protected Access 2). Open system authentication (OSA) offers no security, WEP (Wired Equivalent Privacy) encryption is crackable in less than 60 seconds, and WPA encryption is crackable in hours.

34. What type of attack enables a hacker to forcibly send messages to Bluetooth devices?

A. War driving

B. Bluejacking

C. IV attack

D. Bluesnarfing

Answer: B

Bluejacking enables a hacker to forcibly send message to Bluetooth devices. War driving is used to detect wireless networks. Initiation vector (IV) attacks are used to crack WEP (Wired Equivalent Privacy) encryption. Bluesnarfing enables a hacker to read data from Bluetooth devices.

35. What is the term used to describe the alarm sounded by an IDS (intrusion detection system) based on events it sees in live network traffic that are different from established parameters but which turn out to be benign?

A. True positive

B. False positive

C. True negative

D. False negative

Answer: B

A false positive is when an alarm sounds based on benign events. A true positive is an alarm based on malicious events. A true negative is no alarm due to benign events. A false negative is no alarm but there are malicious events occurring.

36. A signed message or data indicates what?

A. Its source of origin

B. Its compatibility with your operating system

C. Its reliability

D. Its programming quality

Answer: A

A signed message or data indicates its source of origin, not its compatibility, reliability, or quality.

37. LDAP, a standardized protocol that enables clients to access resources within a directory service, is based on what standard?

A. X.509

B. 802.11

C. 160 bits

D. X.500

Answer: D

LDAP (Lightweight Directory Access Protocol) is based on X.500. Certificates are based on X.509. Wireless networking is based on 802.11. 160 bits is the value of an SHA (Secure Hash Algorithm) hash.

38. If you need to give anonymous users the ability to upload files to an Internet site but you don’t wish to grant them the ability to access or even see any files that have been deposited, what do you need to install?

A. S/FTP server

B. SSL server

C. Blind FTP server

D. Authenticated FTP server

Answer: C

Blind FTP gives anonymous users the ability to upload files to an Internet site but doesn’t grant them the ability to access or even see any files that have been deposited. An S/FTP server and an authenticated FTP server eliminate anonymous users. An SSL server is typically used for web traffic security and may require authentication as well.

39. What is the risk calculation metric that measures the number of times an unwanted event might occur within the next year?

A. ALE

B. SLE

C. EF

D. ARO

Answer: D

ARO (annualized rate of occurrence) is the statistical probability that a specific risk may be realized a certain number of times in a year. ALE (annualized loss expectancy) is the potential dollar value loss per year per risk. SLE (single loss expectancy) is the potential dollar-value loss from a single risk realization incident. EF (exposure factor) is the percentage of asset value loss that would occur if a risk was realized.

40. What network device is designed to protect one network from another by filtering traffic?

A. A proxy server

B. A modem

C. A firewall

D. A PBX system

Answer: C

A firewall is a network device designed to protect one network from another by filtering traffic. A proxy server mediates access to untrusted networks for clients in a private network. A modem is used to connect to remote systems. A PBX (private branch exchange) is a network-based telephone system.

41. A link to the network using a modem has what primary difference from a LAN connection?

A. Ability to share files

B. Speed

C. Access to network printers

D. Use of network services

Answer: B

Connecting to the network over a modem rather than a local area network (LAN) cable is different only in terms of speed. A modem-linked system can share files, access network printers, and use network services.

42. What protocol can be used to assist in monitoring the health of a network and to provide a centralized monitoring capability?

A. SMTP

B. TACACS

C. PPTP

D. SNMP

Answer: D

SNMP (Simple Network Transfer Protocol) is used to assist in monitoring the health of a network, and it provides a centralized monitoring capability. SMTP (Simple Mail Transfer Protocol) is used for email. TACACS (Terminal Access Controller Access Control System) is a centralized authentication solution for remote access. PPTP (Point-to-Point Tunneling Protocol) is a VPN (virtual private network) protocol.

43. When an investigator discovers a hard drive that might contain evidence related to a criminal investigation, what is used to create an exact duplicate of that storage device?

A. Hashing

B. Bit-stream image

C. Undelete

D. Graceful shutdown

Answer: B

A bit-stream image is a process used to make an exact hash-matching copy of a storage device. Hashing itself does not create the copy; it can only be used to verify the copy as an exact duplicate. Undelete is not a backup tool, but a potential recovery tool. Graceful shutdown is never part of a forensic investigation as software on the suspect’s system cannot be trusted.

44. When performing system hardening, what is the first step?

A. Install patches and updates.

B. Scan for malicious code.

C. Configure security software.

D. Remove unnecessary elements.

Answer: D

Removing unnecessary elements is always the first step when performing system hardening. All of the other options are steps performed later in the process.

45. Smart cards are often used to store \_\_\_\_\_\_\_\_\_\_\_.

A. Encrypted data files

B. Network account databases

C. Digital certificates

D. User emails

Answer: C

Smart cards are often used to store digital certificates. Encrypted data files, network account databases, and emails are usually too large to fit on a smart card.

46. Which of the following is not a hashing algorithm?

A. SHA-1

B. RC5

C. MD5

D. MD2

Answer: B

RC5 is a symmetric cryptography algorithm. SHA-1, MD5, and MD2 are all hashing algorithms.

47. What is the most important feature of symmetric cryptography?

A. It operates slowly.

B. It is scalable.

C. It uses a shared secret key.

D. It protects integrity.

Answer: C

The most important feature of symmetric cryptography is the shared secret key. Symmetric cryptography is fast, isn’t scalable by itself, and protects confidentiality.

48. Which of the following is not a valid key size for AES?

A. 128

B. 168

C. 192

D. 256

Answer: B

168 isn’t valid for AES (Advanced Encryption Standard)—that’s the key strength of 3DES (Data Encryption Standard). AES uses key sizes of 128, 192, and 256.

49. The benefits of a gas-based fire suppression system include all but which of the following?

A. Can be deployed throughout a facility

B. Will cause the least damage to computer systems

C. Extinguishes the fire by removing oxygen

D. May be able to extinguish the fire faster than a water discharge system

Answer: A

A gas-based fire suppression system can only be used where human presence is at a minimum, since it removes oxygen from the air. Benefits of gas-based fire suppression include causing the least damage to computer systems and extinguishing the fire quickly by removing oxygen.

50. The most effective alternate site is \_\_\_\_\_\_\_\_\_\_\_.

A. Proposed

B. Hot

C. Warm

D. Cold

Answer: B

The most effective alternate site is a hot site. A proposed site is no site at all—it is just a plan to get a site. A warm site is less effective but still a realistic solution. A cold site is a real site but offers an unrealistic solution.

51. Cryptography can be used to provide all but which of the following security features or services?

A. Confidentiality

B. Integrity

C. Availability

D. Non-repudiation

Answer: C

Cryptography is not able to protect and thus provide availability. Cryptography can provide protection for confidentiality, integrity, and non-repudiation.

52. Availability is threatened by what form of attack?

A. Smurf

B. Port scanning

C. Eavesdropping

D. Password cracking

Answer: A

Smurf, a form of denial-of-service attack, threatens or compromises availability. Port scanning and eavesdropping threaten confidentiality. Password cracking threatens authentication.

53. What is a distinctive benefit in deploying an application aware device as compared to a generic firewall appliance?

A. Traffic filtering

B. NAT services

C. Deep packet inspection

D. Network segmentation

Answer: C

Often application aware devices are able to provide deep content inspection and filtering based on their focus on a specific applications and protocols. This makes it a distinct benefit from a generic firewall appliance. Both devices can provide traffic filtering, NAT services, and network segmentation.

54. \_\_\_\_\_ is a networking storage standard based on IP which can be used to enable location independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.

A. Fibre Channel

B. SAN

C. Thunderbolt

D. iSCSI

Answer: D

iSCSI is a networking storage standard based on IP which can be used to enable location independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.

55. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the process of adding new employees to the IAM (Identity and Access Management) of an organization. This process is also used when the role or position of an employee changes or when they are awarded additional levels of privilege or access.

A. Reissue

B. On-boarding

C. Background checks

D. Site survey

Answer: B

On-boarding is the process of adding new employees to the IAM (Identity and Access Management) of an organization. This process is also used when the role or position of an employee changes or when they are awarded additional levels of privilege or access.

56. Which of the following is a formal declaration of the security stance, risks, and technical requirements of a link between two organization's IT infrastructures?

A. MOU

B. SLA

C. ISA

D. BPA

Answer: C

An ISA (Interconnection Security Agreement) is a formal declaration of the security stance, risks, and technical requirements of a link between two organization's IT infrastructures.

57. What form of malware takes a computer system hostage and demands payment in order to release control back to the user?

A. Rootkit

B. Ransomware

C. Trojan horse

D. Logic bomb

Answer: B

Ransomware is a form of malware which aims to take over a computer system in order to block its use while demanding payment. Effectively, it is malware that holds data or an entire computer system hostage in exchange for a ransom payment.

58. When a security consultant is performing a penetration test but is not provided a set of logon name and passwords by the target organization, what form of assessment is being performed?

A. Announced test

B. Non-credentialed test

C. White box test

D. Intrusive test

Answer: B

A non-credentialed test is run without usernames and passwords. An announced test is one where all employees knows it is taking place. A white box test is a full knowledge test. A intrusive test attempts to fully exploit discovered flaws.

59. What is a common organizational and referencing format used by some NoSQL database options?

A. HTML

B. Java

C. JSON

D. LDAP

Answer: C

JSON (JavaScript Object Notation) is a common organizational and referencing format used by some NoSQL database options.

60. What is the purpose of BYOD policies mandating storage segmentation?

A. Lock the device when the user fails to provide their credentials after repeated attempts

B. Enable all data and possibly even configuration settings to be deleted from a device remotely

C. Isolate the device's operating system and pre-installed apps from user installed apps and user data

D. Oversee the installed apps, app usage, stored data, and data access on a device.

Answer: C

Storage segmentation is used to artificially compartmentalize various types or values of data on a storage medium. On a mobile device, the device manufacturer and/or the service provider may use storage segmentation to isolate the device's operating system and pre-installed apps from user installed apps and user data.

61. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a type of ICS (industrial control system). An ICS is a form of computer management device that controls industrial processes and machines.?

A. SCADA

B. SAN

C. DNS

D. Fibre Channel

Answer: A

SCADA (supervisory control and data acquisition) is a type of ICS (industrial control system). An ICS is a form of computer management device that controls industrial processes and machines.

62. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds.

A. Certificates

B. TOTP

C. TPM

D. Trusted OS

Answer: B

TOTP (Time-based One-time Password) tokens or synchronous dynamic password tokens are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds.

63. What is the primary reason to maintain a password history?

A. Monitor account logins

B. Force complexity requirements compliance

C. Provide for legal investigations

D. Prevent password reuse

Answer: D

Password history is an authentication protection feature that tracks previous passwords (by archiving hashes) in order to prevent password reuse.

64. Which of the following depends upon ephemeral keys?

A. Digital certificates

B. Perfect forward secrecy

C. Whole drive encryption

D. Integrity protection

Answer: B

Perfect forward secrecy is a means of ensuring that the compromise of an entity's digital certificates or public/private key pairs do not compromise the security of any sessions keys. Perfect forward secrecy is implemented by using ephemeral keys for each and every session, generated at the time of need, and then only using for a specific period of time or volume of data transfer before being discarded and replaced.

65. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the message sent to a certificate authority from an user or organization to request and apply for a digital certificate.

A. SHA-1

B. OCSP

C. PKI

D. CSR

Answer: D

CSR (Certificate Signing Request) is the message sent to a certificate authority from an user or organization to request and apply for a digital certificate.